

## PELATIHAN PENANGANAN DEFACE PADA PT.CLOUD HOSTING INDONESIA

**Muhammad Fadilah Nurjaman**

Universitas Nusa Putra, Sukabumi, Indonesia

E-mail: [muhammad.fadilah\\_ti21@nusaputra.ac.id](mailto:muhammad.fadilah_ti21@nusaputra.ac.id)

### ARTICLE INFO

**Article history:**

Received :15-11-2024

Revised :-10-12-2024

Accepted: 15-12-2024

**Key words:** Deface attack, WordPress, training, website security

**DOI:** <https://doi.org/10.62335>

### ABSTRACT

*The purpose of this training program was to enhance the skills of interns at PT. Cloud Hosting Indonesia in addressing website defacement issues, particularly on WordPress platforms. The training focused on understanding cyber threats, specifically deface attacks, and hands-on practices in managing index and .htaccess files to improve website security. The results showed that participants successfully learned to identify security vulnerabilities and apply solutions such as disabling unnecessary directory indexing, securing sensitive files, and enforcing HTTPS protocols. This training effectively equipped participants with the necessary skills to prevent and address defacement on WordPress websites.*

### ABSTRAK

Tujuan dari program pelatihan ini adalah untuk meningkatkan keterampilan anak magang di PT. Cloud Hosting Indonesia dalam menangani masalah deface pada website, khususnya pada platform WordPress. Pelatihan ini berfokus pada pemahaman ancaman siber, khususnya serangan deface, serta praktik langsung dalam mengelola file index dan .htaccess untuk meningkatkan keamanan website. Hasil pelatihan menunjukkan bahwa peserta berhasil mengidentifikasi kerentanannya dan menerapkan solusi seperti menonaktifkan pengindeksan direktori yang tidak perlu, mengamankan file sensitif, dan menerapkan protokol HTTPS. Pelatihan ini secara efektif membekali peserta dengan keterampilan yang diperlukan untuk mencegah dan menangani deface pada website WordPress..

## **PENDAHULUAN**

Perkembangan teknologi informasi yang pesat telah mendorong banyak perusahaan untuk memanfaatkan website sebagai salah satu sarana utama dalam menjalankan operasional bisnis dan menjangkau pelanggan. Namun, seiring dengan manfaat yang ditawarkan, risiko keamanan siber menjadi tantangan yang signifikan. Salah satu ancaman yang sering dihadapi adalah website deface, di mana tampilan atau konten website diubah oleh pihak yang tidak berwenang, yang dapat merusak reputasi dan kepercayaan publik terhadap perusahaan.

Deface pada platform WordPress, yang merupakan salah satu CMS (Content Management System) paling populer di dunia, menjadi perhatian khusus karena WordPress banyak digunakan oleh perusahaan kecil hingga besar. Kerentanan ini sering kali terjadi akibat lemahnya pengaturan keamanan, penggunaan plugin atau tema yang tidak terverifikasi, serta kurangnya pengetahuan teknis pengguna dalam melindungi website mereka. Akibatnya, serangan ini tidak hanya berdampak pada perusahaan, tetapi juga pada pengalaman pengguna yang mengakses website tersebut.

PT. CloudHosting Indonesia, sebagai penyedia layanan hosting dan pengelolaan website, sering kali menghadapi masalah terkait deface WordPress pada klien mereka. Untuk mengatasi masalah ini, diperlukan langkah-langkah penanganan cepat dan efektif yang melibatkan perbaikan pada file .htaccess dan pengaturan ulang indexing. Selain itu, keterbatasan jumlah tenaga profesional di bidang keamanan siber di perusahaan ini mendorong perlunya penguatan kemampuan anak-anak magang yang terlibat dalam operasional perusahaan.

Urgensi pelatihan ini didasarkan pada kebutuhan untuk memberikan solusi praktis dan strategis bagi PT. CloudHosting Indonesia dalam menangani insiden deface WordPress secara mandiri. Selain itu, program ini bertujuan untuk meningkatkan kompetensi teknis anak-anak magang sehingga mereka dapat berkontribusi secara langsung dalam menyelesaikan permasalahan tersebut. Dengan demikian, pelatihan ini tidak hanya membantu perusahaan, tetapi juga menjadi bagian dari upaya pengabdian kepada masyarakat melalui pengembangan keterampilan pemuda yang terjun dalam dunia kerja.

## **METODE PELAKSANAAN**

Metode pelaksanaan pengabdian masyarakat ini meliputi serangkaian proses kegiatan yang terstruktur dan ditata secara sistematis untuk mencapai tujuan pelatihan penanganan website deface pada WordPress. Proses pelaksanaan ini terdiri dari beberapa tahap yang saling berkesinambungan, yaitu penyampaian materi dasar, praktik teknis, dan pendampingan langsung, yang dilakukan dengan pendekatan partisipatif dan aplikatif.

Tahap pertama adalah penyampaian materi dasar yang bertujuan memberikan pemahaman kepada peserta mengenai konsep ancaman siber, khususnya deface pada WordPress. Materi disampaikan melalui presentasi interaktif yang mencakup definisi deface, penyebab, dampak, dan contoh kasus nyata. Penyampaian ini dirancang untuk membangun kesadaran peserta akan pentingnya keamanan website.

Tahap kedua adalah sesi praktik teknis, yang fokus pada mengidentifikasi masalah dan melakukan perubahan pada file index dan .htaccess untuk meningkatkan keamanan website serta mencegah akses tidak sah. Dalam sesi ini, peserta diajarkan untuk mengenali jenis-jenis masalah yang sering terjadi akibat konfigurasi yang tidak aman, seperti pengindeksan direktori yang tidak diperlukan, akses terhadap file sensitif, dan kelemahan koneksi.

Tahap akhir adalah pendampingan langsung selama praktik dan simulasi. Pendampingan dilakukan oleh mentor yang memberikan bantuan personal kepada peserta, memastikan setiap individu memahami dan mampu menerapkan teknik yang diajarkan. Selain itu, peserta diberikan evaluasi langsung dan umpan balik spesifik terhadap hasil kerja mereka untuk meningkatkan pemahaman dan keterampilan teknis.

## **HASIL DAN PEMBAHASAN**

Pelatihan penanganan website deface yang dilaksanakan pada PT. CloudHosting Indonesia berhasil dilaksanakan sesuai dengan rencana yang telah ditetapkan. Kegiatan ini melibatkan anak-anak magang sebagai peserta utama dan mencakup tahapan penyampaian materi dasar, sesi praktik teknis, pengaturan indexing, dan pendampingan langsung. Setelah penyampaian materi dasar, peserta menunjukkan peningkatan pemahaman yang signifikan mengenai konsep ancaman siber, khususnya deface pada WordPress. Peserta mampu menjelaskan berbagai jenis serangan deface, faktor penyebabnya, dan dampaknya terhadap perusahaan maupun pengguna website. Melalui diskusi dan studi kasus, peserta juga berhasil mengidentifikasi kelemahan dalam konfigurasi WordPress yang dapat menjadi celah keamanan, seperti plugin yang tidak diperbarui dan lemahnya pengaturan file.

Pada sesi praktik teknis, peserta berhasil mengidentifikasi berbagai potensi masalah yang sering terjadi pada file index dan .htaccess. Simulasi kasus menunjukkan bahwa peserta mampu mengenali tanda-tanda pengindeksan berlebih yang membuka akses ke direktori sensitif, seperti direktori uploads atau file wp-config.php. Selain itu, peserta juga dapat mengidentifikasi masalah pada konfigurasi .htaccess, seperti tidak adanya pembatasan akses file dan direktori atau penggunaan koneksi HTTP yang tidak aman.

Peserta berhasil melakukan perubahan pada file index dan .htaccess untuk meningkatkan keamanan website. Beberapa perubahan yang dilakukan antara lain menonaktifkan pengindeksan direktori dengan menambahkan perintah Options - Indexes, mengamankan file sensitif seperti wp-config.php dengan perintah Deny from All, dan melakukan redirect dari HTTP ke HTTPS untuk memastikan koneksi aman. Selain itu, peserta juga dapat mengedit file robots.txt untuk membatasi pengindeksan oleh mesin pencari terhadap direktori yang tidak diperlukan, serta menyembunyikan file dan direktori yang berisiko.

Selama proses pendampingan langsung, peserta menunjukkan kemampuan praktis yang baik dalam mengatasi masalah keamanan pada WordPress. Dari simulasi serangan deface yang dilakukan, sebanyak 90% peserta berhasil memulihkan kondisi website dengan menerapkan langkah-langkah teknis yang diajarkan. Sisa

peserta yang mengalami kesulitan mendapatkan bimbingan tambahan hingga mereka mampu menyelesaikan permasalahan.

Pelatihan ini memberikan dampak positif, baik bagi peserta maupun PT. CloudHosting Indonesia. Peserta kini memiliki pemahaman dan keterampilan teknis untuk menangani ancaman deface secara mandiri, khususnya dalam pengelolaan file index dan .htaccess. Bagi perusahaan, pelatihan ini membantu menciptakan tenaga kerja magang yang kompeten, yang mampu mendukung operasional perusahaan dalam menjaga keamanan website klien.



Gambar 1 pelatihan penanganan deface

## KESIMPULAN DAN SARAN

Dari hasil pelatihan penanganan website deface pada WordPress yang dilaksanakan di PT. CloudHosting Indonesia, dapat disimpulkan bahwa kegiatan ini berhasil memberikan pemahaman yang mendalam kepada peserta mengenai ancaman siber, khususnya serangan deface. Peserta berhasil mengidentifikasi dan mengatasi masalah pada file index dan .htaccess untuk meningkatkan keamanan website. Dengan adanya sesi praktik teknis dan pendampingan langsung, peserta mampu mengimplementasikan teknik-teknik yang diajarkan secara efektif, seperti menonaktifkan pengindeksan direktori yang tidak perlu, mengamankan file sensitif, dan memastikan koneksi yang aman dengan HTTPS. Secara keseluruhan, pelatihan ini memberikan dampak positif yang signifikan, baik bagi peserta maupun perusahaan, dalam meningkatkan kesiapan menghadapi ancaman siber pada website.

## DAFTAR PUSTAKA

- Pustekom. (2019). Panduan Pengamanan Website dari Serangan Deface. Kementerian Komunikasi dan Informatika Republik Indonesia.
- Sari, M., & Yulianto, A. (2020). Teknik Keamanan pada WordPress: Studi Kasus Penanganan Serangan Deface. *Jurnal Keamanan Sistem Informasi*.

- Gunawan, R., & Hermawan, M. (2021). Penerapan Pengamanan Website Menggunakan .htaccess pada Platform WordPress. Universitas Teknologi Indonesia.
- Pratama, H. (2022). Pengelolaan File Robots.txt dan .htaccess dalam Mengamankan Website dari Ancaman Siber. Jurnal Keamanan Digital.
- Yulianto, B., & Safitri, D. (2021). Manajemen Keamanan Website: Praktik dan Teknologi Terkini. Jakarta: Penerbit Teknologi Informatika.